

JENNIFER LEE TAYLOR (SBN 161368)
JTaylor@mofo.com
STACEY M. SPRENKEL (SBN 241689)
SSprenkel@mofo.com
JOYCE LIOU (SBN 277720)
JLiou@mofo.com
AMANDA D. PHILLIPS (SBN 305614)
APhillips@mofo.com
MORRISON & FOERSTER LLP
425 Market Street
San Francisco, California 94105-2482
Telephone: (415) 268-7000
Facsimile: (415) 268-7522

Attorneys for Defendants/Counterclaimants
UBIQUITI NETWORKS, INC., UBIQUITI
NETWORKS INTERNATIONAL LIMITED,
and Defendant CHING-HAN TSAI

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

SYNOPSYS, INC.,

Plaintiff,

v.

UBIQUITI NETWORKS, INC., UBIQUITI
NETWORKS INTERNATIONAL LIMITED,
CHING-HAN TSAI, and DOES 1-20,
inclusive,

Defendants.

UBIQUITI NETWORKS, INC. and UBIQUITI
NETWORKS INTERNATIONAL LIMITED,

Counterclaimants,

v.

SYNOPSYS, INC.,

Counterdefendant.

Case No. 3:17-cv-00561-WHO (LB)

**DEFENDANTS UBIQUITI
NETWORKS, INC., UBIQUITI
NETWORKS INTERNATIONAL
LIMITED, AND CHING-HAN
TSAI'S BRIEF IN OPPOSITION
TO SYNOPSYS' REQUESTS FOR
INSPECTION**

Date: January 18, 2018

Time: 9:30 a.m.

Place: Courtroom C, 15th Floor

Judge: Honorable Laurel Beeler

INTRODUCTION

Synopsys has approached this case with a single discovery demand from the beginning—to image Defendants’ computers. The very first time the parties spoke about discovery, immediately after the June 14, 2017 case management conference, Synopsys said that it would need to image Defendants’ computers. *No* discovery requests had even been served at the time. Synopsys proposed first imaging the devices of what Synopsys called “the top five users” once Synopsys provided those names to Defendants, but it did not identify them until August 22. A few weeks after that, Synopsys served the 56 requests for inspection at issue here, disregarding its proposal to focus on the “top five users.”

During a November 3 in-person conference regarding the requests for inspection, Synopsys did not address *any* of the objections that Defendants made to the inspection requests and instead focused on how the imaging and inspection should proceed. Synopsys also deflected discussion of the voluminous documents that Defendants had already collected and was reviewing because this case would allegedly turn “entirely” on forensic evidence. Demonstrating ignorance of the burden of its 56 requests for inspection, Synopsys even suggested that as a first step Defendants should collect the multitude of devices at issue in a single room in Taiwan so that its forensic experts could then quickly inspect each device by typing in a few simple commands. This is not the type of inspection it now seeks for Defendant Ching-Han Tsai’s devices.

Synopsys made these repeated demands even while it refused to turn over the “call-home” data that it claims support its allegation of over 39,000 acts of circumvention of Synopsys’ license key system. Synopsys will claim that it could not turn over that data without a protective order, even though the “call-home” data is data that Synopsys acquired *from Defendants*, and that Defendants dragged their feet in negotiating the protective order—which is not at all true. What is true is that the “call-home” data that Synopsys finally produced on December 1 demonstrates that all but 626 of the alleged acts of circumvention took place entirely outside the United States, and that the remaining 626 acts of circumvention were all *completed* outside the United States as well. Thus, while Synopsys has been pressing to image dozens of computers and multiple complex servers, containing highly confidential and attorney-client privileged information, it was

1 withholding from Defendants the very data that show that *none* of the acts of circumvention took
2 place completely within the United States (despite Synopsys’ allegations in its complaint), and
3 that at most, 626 of the acts were initiated from the United States.

4 As discussed further below, the case law is clear that there is *no* DMCA liability for acts
5 such as those recorded by Synopsys’ call-home data. Defendants have already imaged the
6 computers used by Defendant Tsai, who occasionally works from the U.S. and has reason to use
7 the type of electronic design automation (EDA) software tools at the center of this dispute. An
8 inspection of those images will take place as soon as the parties agree to an inspection protocol.
9 Defendants are also willing to make available for inspection the computers of the one U.S.-based
10 engineer, Sheng-Feng Wang, who engaged in a single instance of debugging assistance using
11 Synopsys software. Given that there is no liability in the U.S. for acts of circumvention that
12 occur or are completed outside of the U.S., Synopsys has no basis to image or inspect any of the
13 other computers or servers that it is seeking.

14 BACKGROUND

15 A. Synopsys’ Requests for Forensic Inspection

16 On September 8, 2017, Synopsys served 59 identical requests on Ubiquiti and UNIL to
17 inspect and copy a variety of electronic devices. (Declaration of Jennifer Lee Taylor (“Taylor
18 Decl.”) ¶ 3, Ex. A.) The requests cover forensic inspection of:

- 19 • electronic devices used by nine employees (Request Nos. 1-9);
- 20 • electronic devices used by users of fifteen usernames (Request Nos. 10-24);
- 21 • electronic devices bearing fourteen MAC addresses (Request Nos. 25-38);
- 22 • electronic devices bearing sixteen IP addresses (Request Nos. 39-54); and
- 23 • electronic devices bearing five hostnames (Request Nos. 55-59).

24 On December 1, 2017, Synopsys finally produced a spreadsheet of the “call-home” data that it
25 states provide the basis for these inspection requests. As indicated by that spreadsheet, only 626
26 of the approximately 39,000 call-home events—each of which Synopsys argues is a single act of
27 circumvention under the Digital Copyright Millennium Act (DMCA)—correspond to an “egress”
28 IP address originating from the United States between November 2014 and March 2016. (Taylor

Decl. ¶ 6.) The remaining 38,178 data entries correspond to an egress IP address from Taiwan. (*Id.*) In addition to an egress IP address, each call-home entry identifies a server or host name, username, date, time, and one or more associated MAC addresses. (*Id.*) Synopsys' counsel has represented that the MAC addresses identified by the call-home data correspond to computers that have Synopsys software on them and that transmit data back to Synopsys when a counterfeit key is detected. (*Id.*)

B. Relationship of Requested Devices to the United States

Employee Computers. Synopsys' inspection requests encompass *at least* 26 different employee computers.¹ Not only are most of these devices physically located in Taiwan, most have no connection whatsoever to computer systems in the United States because they are used by team members who reside in Taiwan, work in UNIL's Taipei office, and perform their daily work on UNIL's local computer networks in Taipei. The team consists of 18 engineers with different roles on a discrete project to design a semiconductor chip for one of Ubiquiti's products. (Declaration of Ching-Han Tsai ("Tsai Decl.") ¶ 2.) Defendant Tsai was hired first as the project lead in September 2013, and was responsible for building the rest of the team. (*Id.*) Due to a faster hiring process in Taiwan, Tsai chose to base the team, with one exception, at Ubiquiti's major research and development location in UNIL's Taipei office, and relocated himself from the U.S. to Taiwan to be in the same location as other team members. (*Id.*)

Of the 17 current team members in UNIL's Taipei office, just one—Tsai—travels from Taiwan to the U.S. on occasion for work or to visit family, and would have need to use EDA software tools regularly while in the United States. (*Id.* ¶¶ 13-14.) One other team member, Sheng-Feng Wang, is based in the U.S. but has no need to use EDA software tools in his regular

¹ Defendants emphasize "at least" because Synopsys' requests, specifically Request Nos. 39-54 for any electronic devices "bearing" fifteen different IP addresses, potentially capture hundreds and hundreds of Defendants' computers—not just those used by the relevant custodians whom Defendants identified in interrogatory responses—that may have used any one of the corporate IP addresses at any given point in time, but that have no relevancy other than use of a common IP address at a hundred-plus person site. Defendants timely objected to these requests as vague, overly broad, and unduly burdensome. (*See* Taylor Decl. ¶ 3, Ex. B.) Synopsys never conferred regarding those objections. (*Id.* ¶ 4.) Defendants request that the Court decline to allow *any* inspection that would be covered by Request Nos. 39-54 based on those objections.

1 work given his project role. (Declaration of Shen-Feng Wang (“Wang Decl.”) ¶¶ 2, 6.) While
2 the entire team has access to two shared username accounts on UNIL’s computer systems, only a
3 select few have a reason to access EDA software for designing application specific integrated
4 circuits (ASIC), let alone the technical skills to use such software or an occasion to use it from the
5 United States. (Tsai Decl. ¶ 17.)

6 **Server Devices.** In addition to employee devices, Synopsys’ inspection requests identify
7 MAC addresses and host names for several computational servers and virtual machines that are
8 not only located in Taiwan, but also contain the only copies of EDA software that would have
9 been used by the current team members whose role is to design and test ASIC chips. (*See id.*
10 ¶¶ 7-13.) All EDA software used by the team is located on a storage array in UNIL’s Taipei
11 office, and accessible only via three computational servers and the virtual machines on them, also
12 in Taiwan, which are networked with the storage array. (*Id.* ¶ 12.) This local area network is
13 remotely accessed by ASIC design team members using their individual laptops and computers.
14 (*Id.*) Because of the nature of ASIC design work, including the processing resources that are
15 required for running simulations, this local network of computational servers and virtual
16 machines in UNIL’s Taipei office is separate from Ubiquiti’s IT infrastructure, including the rest
17 of UNIL’s IT infrastructure in Taiwan. (*Id.*)

18 Any ASIC design team member who needs to access EDA software on the storage array
19 does so by first logging into his computer and connecting remotely to the computational servers
20 to initiate simulations. (*Id.* ¶ 13.) Those computational servers, and any virtual machines
21 residing on them, then use the EDA software located on the storage array to conduct the
22 simulations. (*Id.*) Because of how UNIL’s computer networks and servers are configured, there
23 is no need for any EDA software or license key to be loaded on an employee computer. (*Id.*)

24 **ARGUMENT**

25 **I. U.S. COPYRIGHT LAWS APPLY ONLY TO ACTS THAT ARE COMPLETED** 26 **WITHIN THE UNITED STATES**

27 The purported purpose of Synopsys’ requests to forensically inspect Defendants’
28 electronic devices—to find evidence of forensic artifacts of license key generators, use of piracy

1 websites, external drives, and user profiles (*see* Dkt. No. 99 at 2)—is only relevant to Synopsys’
2 first claim of circumvention of Synopsys’ license-key system under the DMCA, 17 U.S.C.
3 § 1201(a)(1). This section of the DMCA makes it a violation to “circumvent” a technological
4 measure that effectively controls access to a copyrighted work, by descrambling a scrambled
5 work, decrypting an encrypted work, or otherwise avoiding, bypassing, removing, deactivating, or
6 impairing the technological measure. 17 U.S.C. § 1201(a)(1), (3). Synopsys asserts thirteen
7 copyrighted software programs that are access-controlled by Synopsys’ license-key system, and
8 Synopsys alleges that Defendants circumvented the license-key system through use of
9 “counterfeit” license keys in violation of the DMCA. (Dkt. No. 73 ¶¶ 24-26, 28.) No other claim
10 asserted by Synopsys justifies a burdensome forensic inspection of Defendants’ devices for
11 forensic artifacts of software usage, nor has Synopsys asserted that one is necessary for any other
12 claim. Discovery on Synopsys’ other claims may be addressed through document production.

13 As explained below, Defendants believe the requested forensic inspection, which would
14 encompass at least 26 employee computers and 3 servers located in Taiwan, goes well beyond the
15 scope of this action, and seeks discovery of entirely irrelevant information, because liability under
16 the DMCA can only extend to acts of circumvention that are completed within the United States.

17 **First**, it is black letter law that U.S. copyright laws do not impose liability for
18 extraterritorial acts. In *Subafilms*, the Ninth Circuit confirmed the longstanding principle that
19 U.S. copyright laws do *not* reach acts of infringement that occur outside the United States.
20 *Subafilms, Ltd. v. MGM-Pathe Commc’ns Co.*, 24 F.3d 1088, 1095-96, 98 (9th Cir. 1994) (en
21 banc) (“The undisputed axiom . . . that the United States’ copyright laws have no application to
22 extraterritorial infringement predates the 1909 Act, . . . and, . . . the principle of territoriality
23 consistently has been reaffirmed.”) (citations omitted). Faced with a U.S. defendant who, from
24 the United States, authorized a foreign company to distribute copyrighted materials outside the
25 United States, the Ninth Circuit stated that the defendant’s “mere authorization of acts of
26 infringement . . . [that] occur entirely outside of the United States does not state a claim for
27 infringement under the Copyright Act,” and found the defendant not liable. *Id.* at 1099.

28 Similarly, in *Allarcom*, the Ninth Circuit found that a U.S. defendant was not liable under

1 the Copyright Act for committing a part of an act of infringement that *began* in the United States
2 and culminated overseas. *Allarcom Pay Television, Ltd. v. Gen. Instrument Corp.*, 69 F.3d 381,
3 387 (9th Cir. 1995). Citing its prior *Subafilms* decision, the Ninth Circuit stated:

4 We held that in order for U.S. copyright law to apply, at least one
5 alleged infringement must be completed *entirely within* the United
6 States, and that mere authorization of extraterritorial infringement
7 was not a completed act of infringement in the United States.
8 *Subafilms*, 24 F.3d at 1094, 1098. In this case, defendants either
9 *initiated* a potential infringement in the United States by
10 broadcasting the Showtime signal, which contained copyrighted
11 material, or defendants authorized people in Canada to engage in
12 infringement. In either case, the potential infringement was only
13 *completed* in Canada once the signal was received and viewed.
14 Accordingly, U.S. copyright law did not apply, and therefore did
15 not preempt Allarcom's state law claims.

16 *Allarcom*, 69 F.3d at 387 (emphasis added).

17 As *Subafilm* and *Allarcom* show, liability does not exist if only *some* part of a violative act
18 was initiated within the United States. Rather, the violative act must be *completed* within the
19 territorial boundaries of the United States for U.S. copyright law to apply, as a contrary result
20 would displace foreign copyright laws and cause potential international discord. See *Subafilms*,
21 24 F.3d at 1097-98 (noting an application of U.S. law to copyrighted materials distributed
22 exclusively by national citizens in a foreign country undermines the spirit of national treatment
23 under the Berne Convention); cf. *Robert Stigwood Grp. Ltd. v. O'Reilly*, 530 F.2d 1096, 1100-01
24 (2d Cir. 1976) (no liability for performances of copyrighted work in Canada merely because
25 performers assembled and arranged all necessary elements in the United States). These cases are
26 clear that the site of the completed violative act determines which country's copyright laws apply,
27 and it is irrelevant whether the initiating act is integral to the final completed act.

28 **Second**, to assess whether acts involving computer transmissions over the Internet may
create liability under U.S. copyright law, the Ninth Circuit has derived a "server test" for
determining the site of the alleged violation. See *Perfect 10, Inc. v. Yandex N.V.*, 962 F. Supp. 2d
1146, 1153 (N.D. Cal. 2013). That test "makes the hosting website's computer [which stores
electronic information and serves that information to the user], rather than the search engine's
computer [which merely frames electronic information for the user but does not store it], the situs

1 of direct copyright infringement liability.” *Id.* (citing *Perfect 10, Inc. v. Amazon.com, Inc.*, 508
2 F.3d 1146, 1159-60 (9th Cir. 2007)). In *Yandex*, the defendants moved for summary judgment on
3 the plaintiff’s direct copyright infringement claim based on acts of infringement concerning
4 content hosted on servers in Russia. Applying the Ninth Circuit’s server test, the *Yandex* court
5 granted summary judgment for the defendants, holding that the hosting of images on Russian
6 servers are extraterritorial acts that are not actionable under U.S. copyright law. 962 F. Supp. 2d
7 at 1152-53. Notably, the court rejected the notion that U.S. copyright liability may arise merely
8 because an image could be downloaded from a foreign server by a user in the United States as
9 “[s]uch a principle would destroy the concept of territoriality inherent in the Copyright Act for
10 works on the internet.” *Id.* at 1153. As *Yandex* illustrates, even activities conducted over the
11 Internet must be identified by where they occur—i.e., within the borders of the country of origin
12 or destination—for purposes of determining which country’s copyright laws govern.

13 **II. ACTS INITIATED IN TAIWAN AND COMPLETED ON TAIWAN SERVERS** 14 **ARE NOT ACTIONABLE UNDER THE DMCA**

15 Synopsys has asserted a claim of circumvention under the Digital Millennium Copyright
16 Act, a copyright law that implemented two World of Intellectual Property Organization (WIPO)
17 treaties to which the U.S. is a signatory—the WIPO Copyright Treaty and WIPO Performances
18 and Phonograph Treaty—and created U.S. remedies for circumvention conduct.²

19 As an initial matter, Synopsys has previously suggested that extraterritoriality
20 jurisprudence under the Copyright Act does not extend to the DMCA. This is contrary to both
21 *Subafilms* and lower court authority that have held that U.S. copyright laws, of which the DMCA
22 is one, do not have extraterritorial effect. *See, e.g., M Seven Sys. Ltd. v. Leap Wireless Int’l, Inc.*,
23 2014 WL 12026065, at *6 (S.D. Cal. June 4, 2014) (the DMCA does not apply if the alleged
24 violation occurred in a foreign nation). Furthermore, the Supreme Court has held that courts must
25 “assume that Congress legislates against the backdrop of the presumption against
26 extraterritoriality,” and must presume a federal statute concerns only domestic activities absent
27 “the affirmative intention of the Congress clearly expressed.” *EEOC v. Arabian Am. Oil Co.*, 499

28 ² See http://www.wipo.int/copyright/en/activities/internet_treaties.html.

1 U.S. 244, 248 (1991) (citation omitted). Here, the statutory language lacks any indication of
2 Congress' intent to reach beyond U.S. borders, as confirmed by text relating to U.S.-only sales of
3 copy-control circumvention technology in 17 U.S.C. § 1201, and the legislative history "further
4 supports the contention that the DMCA was seen [by Congress] as a protectionist, nationalistic
5 law that only applied territorially." Adam D. Fuller, *Extraterritorial Implications of the Digital
6 Millennium Copyright Act*, 35 Case W. Res. J. Int'l L. 89, 111-112 (2003). The territorial limit of
7 the DMCA is therefore presumed.

8 Because the DMCA does not apply to extraterritorial activity, Defendants cannot be held
9 liable for any alleged acts of circumvention that were initiated on employee computers in *Taiwan*
10 and completed on servers in *Taiwan*, which did not involve any computer systems in the United
11 States. Under Ninth Circuit law, Defendants are not liable because these alleged acts occurred
12 **entirely in Taiwan**. See *Subafilms*, 24 F.3d at 1099. According to Synopsys' data, 38,178 of the
13 approximately 39,000 call-home entries are associated with (i) an egress IP address from Taiwan,
14 and (ii) a host name and MAC address corresponding to a computational server or virtual
15 machine in Taiwan. (See Taylor Decl. ¶ 6, Tsai Decl. ¶¶ 6-9.) This is no surprise as only *one*
16 engineer on the entire project team, Sheng-Feng Wang, is based in the U.S., and only Defendant
17 Tsai in UNIL's Taipei office regularly travels to and works from the U.S. (Wang Decl. ¶ 2, Tsai
18 Decl. ¶ 14.) Because these 38,178 alleged acts of license-key circumvention initiated from
19 Taiwan are not actionable in the U.S., Synopsys has no basis to forensically inspect the UNIL
20 employee computers that might account for such wholly extraterritorial acts. Defendants have
21 submitted declarations from fifteen of the sixteen UNIL engineers verifying that each person lives
22 and works in Taiwan and had no reason to access Synopsys software using his work computer in
23 the U.S. (either because the employee has never traveled to the U.S. or had no need for it).³

24
25 ³ The sixteenth UNIL employee (a software engineer based in Taipei) is on vacation this
26 week. He traveled to the U.S. only one time for work in August 2017, after the filing of the
27 lawsuit. (Declaration of Hayley Nivelle ¶ 6.) Defendants have submitted a separate declaration
28 regarding two project team members no longer employed UNIL who, like the current UNIL
engineers, worked in the Taiwan office. (*Id.* ¶¶ 3-5.) One never traveled to the U.S. for work; the
other traveled to the U.S. in March 2014, which predates the period of "calls home" from the
United States according to Synopsys' data, meaning that employee could not have used Synopsys
software in the U.S. (See Taylor Decl. ¶ 6.)

1 These employees' computers, totaling 26 or more, should thus be excluded by the Court from any
2 required forensic inspection.

3 **III. ACTS INITIATED IN THE UNITED STATES AND COMPLETED ON TAIWAN**
4 **SERVERS ARE NOT ACTIONABLE UNDER THE DMCA**

5 Synopsys' call-home data makes it clear that all of the remaining 626 alleged acts of
6 circumvention were, at most, only *initiated* in the U.S. and then completed on servers in Taiwan.
7 Under *Allarcom*, there is no liability where an act is initiated in the U.S. but *completed* in another
8 country. *Allarcom*, 69 F.3d at 387. Further, applying the Ninth Circuit's "server test" to these
9 alleged acts of circumvention initiated in the U.S., it is clear that the site of the violative act (the
10 alleged use of "counterfeit" license keys to circumvent Synopsys' license-key system) are the
11 servers that actually hosted Synopsys software—because that is the only place where the act
12 *could* be completed—and not an employee computer that remotely initiated the act or where the
13 displayed results could be viewed. *See Perfect 10*, 508 F.3d at 1159-61 (noting "it is the website
14 publisher's computer, rather than Google's computer, that stores and displays the infringing
15 image," and "Google's search engine communicates HTML instructions that tell a user's browser
16 where to find full-size images on a website publisher's computer, but Google does not itself
17 distribute copies of the infringing photographs"); *Yandex*, 962 F. Supp. 2d at 1152-53 (hosting of
18 infringing images on Russian servers are extraterritorial acts that are not actionable under U.S.
19 copyright law).

20 Synopsys' call-home data includes 14 MAC addresses. (Taylor Decl. ¶ 6.) A MAC
21 address is a unique identification number for an electronic device. (Tsai Decl. ¶ 7.) The 14 MAC
22 addresses correspond to three UNIL servers located in Taiwan, and to virtual machines located on
23 those servers (*see* Tsai Decl. ¶¶ 7-9), but only 3 of the 14 MAC addresses appear in the entries
24 where "USA" is listed as the country. (Declaration of Shahin Nazarian ("Nazarian Decl.") ¶ 8.)
25 The three UNIL servers have never left UNIL's facility in Taiwan. (Tsai Decl. ¶ 11.) Notably,
26 the MAC addresses for Tsai's own computers do not appear at all in the call-home data, including
27 in the call-home data for entries where "USA" is listed as the country, even though Tsai used his
28 laptop while in the U.S. to initiate simulations remotely in Taiwan. (*Id.* ¶¶ 10, 14-15.) This is not

1 surprising because, as explained by Defendants’ expert, Professor Shahin Nazarian of the
2 University of Southern California Viterbi School of Engineering, the MAC addresses in the call-
3 home data identifying “USA” as the country are for servers in Taiwan. (Nazarian Decl. ¶¶ 7-11.)
4 Given this, there is no support for a claim that *any* Synopsys software was installed on Tsai’s
5 computers. (*Id.* ¶ 12.) Likewise, there is no support for a claim that Synopsys’ software was
6 installed anywhere other than on servers and virtual machines in Taiwan. Thus, the facts here are
7 analogous to those in *Allarcom*, where the Ninth Circuit held that there was no liability under the
8 U.S. copyright laws where transmissions were initiated or authorized from the U.S., but
9 *completed* in Canada. *Allarcom*, 69 F.3d at 387.

10 Nevertheless, even though there is no reason to believe that they ever had Synopsys
11 software installed on them, Defendants have already imaged Tsai’s computers and will make
12 them available to Synopsys for inspection as soon as the parties agree to an inspection
13 protocol. (Taylor Decl. ¶ 5.) Defendants are willing to do the same for the computers of Sheng-
14 Feng Wang, the only team member based in the U.S., not because Synopsys has come forward
15 with any justification for believing that they ever had Synopsys software installed on them, but
16 because inspecting them will prove that they did not. There is absolutely no justification for
17 inspecting any other devices based upon claims that Synopsys’ software was used from the
18 United States. It is Synopsys’ burden to show that it is seeking discovery “*relevant* to any party’s
19 claim or defense *and* proportional to the needs of the case.” Fed. R. Civ. P. 26(b)(1) (emphasis
20 added). It has not and its requests for further imaging or inspection should be denied.

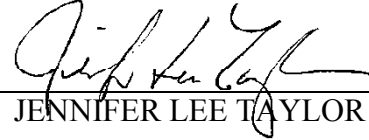
21 CONCLUSION

22 Defendants believe Judge Orrick will rule on summary judgment that none of the 39,000
23 alleged license-key circumventions that happened in Taiwan—as could only have happened since
24 Synopsys’ software was hosted on servers in Taiwan—is actionable under the DMCA. Thus,
25 Defendants believe that there is no basis to permit Synopsys to forensically inspect 29 or more
26 employee computers and servers located in Taiwan, considering the immense burden and expense
27 of coordinating such inspection, and the disproportionality of the requests based on their marginal
28 value to the case.

1 Dated: December 29, 2017

JENNIFER LEE TAYLOR
STACEY M. SPRENKEL
JOYCE LIU
AMANDA D. PHILLIPS
MORRISON & FOERSTER LLP

2
3
4
5 By:


JENNIFER LEE TAYLOR

6
7 *Attorneys for*
8 *Defendants/Counterclaimants*
9 UBIQUITI NETWORKS, INC.,
10 UBIQUITI NETWORKS
11 INTERNATIONAL LIMITED, and
12 *Defendant* CHING-HAN TSAI
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28